AR-009-224

DSTO-RR-0033

The DORIC Program: Network Management

Paul Berry and Wolf Getto

DEPARTMENT ◆ OF DEFENCE
DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

The Doric Program: Network Management (U)

Paul Berry and Wolf Getto

Communications Division
Electronics and Surveillance Research Laboratory

DSTO-RR-0033

ABSTRACT

A characteristic of network management today is its growing diversity in the face of increasing network complexity. For one thing, we are beginning to think of electronic communication networks in terms of 'information networks', comprising networked transmission systems and networked information systems. Secondly, what used to be thought of as simply network management is now splitting into two main capabilities: network management and service management. The complexity of evolving civil network management standards demands that serious consideration be given to the task of understanding how to integrate the management of Defence networks for improved efficiency, interoperability, and flexibility of service provision.

RELEASE LIMITATION

Approved for public release

DEPARTMENT OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury, South Australia 5108 Australia

Telephone: (08) 259 5555
Fax: (08) 259 6549

AR-009-224
September 1994

APPROVED FOR PUBLIC RELEASE

The Doric Program: Network Management

EXECUTIVE SUMMARY

A characteristic of network management today is its growing diversity in the face of increasing network complexity. For one thing, we are beginning to think of electronic communication networks in terms of 'information networks', comprising networked transmission systems and networked information systems. Secondly, what used to be thought of as simply network management is now splitting into two main capabilities: network management and service management.

The complexity of evolving civil network management standards demands that serious consideration be given to the task of understanding how to integrate the management of Defence networks for improved efficiency, interoperability, and flexibility of service provision. In a military environment, specific issues arise which need to be addressed such as the security of network management information, the reliability of critical network management software, and the survivability of the network management system itself. In conjunction with civil network operators, a goal network management functional architecture needs to be identified, and a migration strategy developed which is consistent with their plans and military requirements. This should encompass issues arising from the need for each network to access the other's data and control its services so as to manage services end-to-end and optimise operations globally.

Authors

Paul Berry
Communications Division

Paul is a senior research scientist with interests in performance modelling of communication systems.

Wolf Getto
Communications Division

Wolf is an engineer with interests in software engineering and network management.

Contents

Abbreviations

ACP	Association Control Protocol
ACSE	Association Control Service Element
ATM	Asynchronous Transfer Mode
CMIP	Common Management Information Protocol
CMISE	Common Management Information Service Element
CORBA	Common Object Request Broker Architecture
DME	Distributed Management Environment
DOMS	Distributed Object Management Systems
DPE	Distributed Processing Environments
IAB	Internet Architecture Board
IN	Intelligent Networks
INA	Information Networking Architecture
IP	Internet Protocol
ISO	International Standards Organisation
ITU	International Telecommunications Union
LME	Layer Management Element
LPP	Lightweight Presentation Protocol
MIB	Management Information Base
OAM&P	Operations, Administration, Maintenance and Provisioning
OMG	Object Management Group
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSS	Operations Support System
ROP	Remote Operations Control Protocol
ROSE	Remote Operations Service Element
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TINA	Telecommunications Information Networking Architecture
TMN	Telecommunications Management Network
UDP	User Datagram Protocol

1. Introduction

Network management in its broadest sense encompasses both the human and automated decision making processes involved in all stages of the life cycle of a communications network, including planning, design and operation. The automation of the decision-making processes, either in real-time or off-line, for the purpose of optimising the performance of an ATM-based military network is the subject of the accompanying document entitled "The DORIC Program: ATM Network Performance". The objective of DSTO's research is to devise suitable traffic control algorithms and demonstrate their efficacy in rendering an ATM-based military network efficient in operation, survivable, and able to guarantee quality of service to high priority users, given a dynamic topology, fragile transmission links, and possible correlations in traffic loading. If the stated benefits of ATM are to be achieved, namely integration of users, networks and services, and economies of scale in using global civil standards, then performance considerations are critical to its adoption in a military environment

Decision-making, however, is not the only aspect of importance. Decisions depend on the provision of correct and timely information, and this requires a supporting infrastructure for observing, communicating, recording and controlling the state of the network. This could be a human infrastructure for coordinating the deployment of a tactical network, for example, which would require an appropriate command structure. Equally, it could mean an automated system for monitoring and controlling network operations on a short timescale, with a human operator, backed up by a suite of off-line performance management tools, for handling problems arising on a longer timescale. This report is concerned with network management in its narrower sense of an automated system for managing the flow and processing of network status and control information.

As networks of computers and communications equipment expand and pervade more and more facets of information processing—as they extend and deepen their interconnectivity and interoperability across more and more boundaries (geographical, political, bureaucratic, business etc.)—the problem of how best to manage the mushrooming complexity becomes increasingly pressing. Technologists tend to share a common first approach to the compartmentalisation of the problem, by dividing management into two groups:

- *Network Management*. Responsible for network operation, maintenance and service provisioning; dealing with statistics, status, configuration and fault reporting.
- *Service Management*. Responsible for the management of services and resources that are allocated in the course of the control of calls and connections.

This division is motivated in part by the realisation that there are advantages in designing management architectures in alignment with architectures that are emerging in related technologies such as Intelligent Networks (IN), Distributed Processing Environments (DPE) and Distributed Object Management Systems (DOMS).

After discussing the issue of management complexity in section 2 for the purposes of arriving at a better understanding of the extent of the problem, we turn to the difference between network management and service management in section 3. In section 4 we take a brief look at developments in management architectures.

2. Complexity

The widely used term *telecommunications* reflects the hybrid technological nature of modern communications infrastructures. Originally, it referred to telegraphic and telephonic signalling by line or radio. This is what used to pass for communications transmission, and in fact these are still widely used today. However, the meaning of the term telecommunications is loosening as technology mushrooms. Nowadays there are a wide and growing variety of transmission techniques. For example, a single telephone call within one continent (let alone across continents) may span transmission systems such as cellular radio, satellite, microwave bearer, cable, and optical fibre. In the case of the Australian military there is also a large dependence on HF radio. So, personal communications is no longer a choice of telegraphy or telephony. But parallel to the expansion of technology there has also been some consolidation. Specifically, the proliferation of computers is blurring the distinction between data and voice systems. For many years now people have interacted with electronic mail and file transfer via computer communications equipment that often made use of telephone equipment (its media and its switches) while remaining logically separate from them. With new communications techniques, however, such as *collaborative working*,[1] the boundary between computer and telephone is beginning to merge. These tend to have a *multi-media* characteristic: that is, communications involves a session of several communications sources, such as voice, data, and video. Furthermore, with the expanding digitisation of communication systems, underlying transmission systems are evolving that serve a wide variety of information sources: voice, video and bursty computer communications traffic alike. The influence of modern information technology and digital electronics has been such that, increasingly, when we look at what is being carried by an information transport system, all we are aware of is data. Asynchronous Transfer Mode (ATM) is one such system that has been designed specifically to cater for multi-media communications—in fact the size of ATM cells was arrived at as a compromise between the different requirements of traditional data communication systems on the one hand and voice communication systems on the other.

Therefore, while transmission technology may once have been useful in classifying communication systems, today this is no longer a convenient criterion for the purposes of designing management systems. In fact, standard control interfaces, such as the association-oriented protocols of the Open Systems Interconnection (OSI) network management model or the connectionless message passing of the management protocol defined by the Internet community, allow us to consider a variety of transmission systems as simply information

[1] Collaborative working refers to communication platforms based on workstations (small graphic-intensive computers) where work sessions are established that support a common, shared work-space. Activity at one platform is rapidly reflected at other platforms such that two or more people are able to interactively work on the same product (e.g. a drawing, document, database, etc.)

channels with different characteristics (e.g. delay, capacity), while dealing with each of them via exactly the same mechanism to achieve configuration and control. Gone are the days of building separate network management systems for different transmission systems. At this level of the network, things are becoming simpler and neater. How is it then that the management of multi-media systems is becoming more, and not less, complicated? The answer is that there has been an explosion of activity in the development of information technologies. Networking complexity has been pushed up from the transmission systems to the information processing systems.

We can identify four main factors that have contributed to the growth in network complexity:

- increasing heterogeneity of information processing platforms;
- increasing interworking of information systems;
- maturation of distributed processing;
- multi-media communications.

Users of information networks are demanding that their systems accommodate a greater variety of communications and computer equipment from a greater variety vendors. They are demanding that their systems adhere to open standards to facilitate the interworking of such equipment and the interworking of entire information processing *domains* across a wide variety of physical, organisational and logical boundaries. Domains may be bounded by geography, nation, province, company, government department, military service, security classification etc. Increasingly, the huge parallelism of highly interconnected computer networks and multiprocessor computer architectures is leading to a growth in the development of distributed processing technology. Also, information itself is proliferating as witnessed by the growth in development of multi-media communications. Increasingly, users are demanding access to a greater richness of information for transmission and processing. People using machines to communicate are coming to expect a greater diversity of functionality—electronic mail, voice mail, stored-program voice control (e.g. PABX's), video conferencing, to name a few—while also expecting that such systems cater for the nuances and subtleties of direct person-to-person communication. Meanwhile, research into *virtual reality* seeks to provide a total sensory interface between human and machine.

Therefore, let us think in terms of *information networks* rather than the traditional telecommunication networks: the intention being to suggest that, increasingly, the electronic communication networks of today comprise networks of both telecommunication systems and information processing systems, which are massive in terms of both the expanse of their interconnectedness and the depth of their interworking. By corollary, the task of managing such networks becomes one of management of transmission systems alongside management of the information being transmitted. This is what we mean by making the distinction of network management and service management.

3. Communication Systems and Services

The basic approach to information network management is heavily indebted to the work carried out by the standards bodies: the International Telecommunications Union (ITU), the International Standards Organisation (ISO) and the Internet Architecture Board (IAB). From ITU we have the CCITT M series recommendations *Principles for a Telecommunications Management Network* which defines the management architecture abbreviated as TMN. It embraces a general network model of three super-imposed *planes*:

- *User Plane*. The lowest layer, where the connections between access points to the network are handled. It handles the transmission and switching to provide network/service access to the user.
- *Control Plane*. The middle layer, where logic and data reside which are necessary to control calls and services in real-time.
- *Management Plane*. The highest layer, where operation, maintenance and provisioning of network and services is performed.

Typically, the management and control planes are thought of as hosting network 'intelligence'. Where the management plane deals with permanent data handling and the control plane deals with call-related data handling, the user plane is only concerned with information transfer. Therefore, management of information networks focuses on the upper two layers.

As we shall see in the following section, the entities of a TMN architecture, referred to as *functional blocks*, interface in the management plane with the *network elements* that operate in the control plane—typically, using either the association-oriented protocols defined by ISO or the connectionless message passing protocols of IAB. Meanwhile, the *functional entities* of the evolving IN architecture (analogous to TMN functional blocks) are (predominantly) designed to interface with the *signalling systems* of the control plane. In very simple terms, the management plane is the province of the TMN architecture, whereas the IN architecture is primarily concerned with the control plane. In actual fact however, the situation is a little more complicated since both architectures contend for responsibility for service management, which they do from slightly different perspectives. (Also, as mentioned above, TMN is concerned with the control plane through its relationship with network elements.) From the point of view of TMN, service management focuses on the provisioning and maintenance of telecommunications network resources in a fairly 'global' fashion. That is, it emphasises services that are invoked by callers the same way within a given community, and in a way that remains fairly static from call to call. Take, for example, the allocation to a business of call-accounting facilities. Another example might be a traffic management service that guarantees a business a given quality of service—but is incapable of providing the same service to calls *terminating* at that site, or of distinguishing *between* calls.[2] IN takes a different approach to service management—one that handles services in a fairly 'individualised' fashion. Being as tightly responsive as it is to the control of calls and connections, IN is in a position to manage

[2] This is not to say that a TMN system could not be designed to manage such an extended service, but only that a TMN architecture might not be the best practical solution (as compared with IN for instance).

services that are invoked on a call by call basis that is sensitive to the context of the call. Take, for example, the allocation to a business of a telephone number that is available to callers in any state within a country, but where calls are routed to the business facility in closest proximity to the caller—hence Bob in Sydney and Sue in Melbourne both dial the same number for a pizza, but Bob is connected to a shop in Pitt St. while Sue is connected to a shop in Spring St.

The blurring of boundaries arises in as much as TMN is mainly associated with the management plane whereas IN is notionally associated with the control plane. In fact, the two evolving architectures are beginning to 'spread out' and straddle both planes. Fortunately, communication and information technologists, bothered by the redundancy and untidiness of this situation, are working towards a merging of the two architectures, in recognition of the dichotomy of management into network management and service management. It is this process that has motivated an integrated approach to the problem of information network management in the form of the Telecommunications Information Networking Architecture (TINA).[3] We explore this process in greater depth in the following section, and also address how it is simultaneously being influenced by distributed system technologies which are pulling information networks in the direction of: distributed processing, applications portability and object-orientedness.

4. Management Architectures

Looking at network management and service management separately, we go on to look at moves to consolidate the two management streams into an integrated information network architecture. Towards this end, we look at the way in which network management architectures exploit the communications and management protocols of ISO and IAB. We then look at how ATM maps onto this. Also, we look at the way in which IN caters for the management of services.

This will then lead us to a very brief summary of emerging distributed system technologies such as Bellcore's Information Networking Architecture (INA), with its associated concept of *service segment* and delivery, ITU's Open Distributed Processing (ODP) reference model, which aims at a standardised framework for DPE's, and the Open Software Foundation's (OSF) Distributed Management Environment (DME), which serves as an example of a DOMS that is a working architecture with growing industry support.

But to begin with, let us look at the main functional blocks/entities of TMN and IN in order become better acquainted with the main roles of these architectures and their relationship with the management and control planes. In the process we will also become more familiar with the relationship between the two planes themselves.

[3] A consortium formed in 1992 by Bellcore, BT and NTT.

TMN functional blocks:

- *Operation Systems Function* (OSF): processing of telecommunication management information for the purpose of monitoring, supervising, provisioning etc. the information network and the services it offers;
- *Network Element Function* (NEF): outside of the TMN, but communicating with it, and providing the necessary functions to support the telecommunications services offered by the network (switching and signalling, call and connection setup etc.);
- *Workstation Function* (WSF): communication with the management operator, providing interpretation and presentation of management information;
- *Mediation Function* (MF) and *Q Adapter Function* (QAF): mediation and adapter functions to convert information and protocols in order to enable communication between different function blocks.

IN functional entities:

- *Call Control Agent Function* (CCAF): interface allowing users to access call and service processing;
- *Call Control Function* (CCF): real time call control for the establishment of calls and connections during the execution of a particular service requested by a user;
- *Service Control Function* (SCF): processing of intelligent networking logic as invoked by call control and responding by directing call control and/or organising the connection of specialised resources to a user;
- *Specialised Resource Function* (SRF): network resources (pre-recorded announcements, conference servers etc.) allocated to users by service control during call control and service invocation;
- *Service Management Function* (SMF): deployment and provision of services and the necessary updating of service-related data via the management of service control;
- *Service Management Agent Function* (SMAF): interface between management operators and service management;
- *Service Creation Environment Function* (SCEF): definition, development and testing of services and subsequent input to service management.

In general terms, IN is concerned with network services in terms of the control of calls and connections in association with the control of specialised resources. Consequently, a large part of the functionality of IN is taken up with service management. Therefore, IN is active in both the control plane and the management plane; and as regards the latter, it focuses on the management of the services of a network in terms of *value added* functionality that it is supported by a signalling and switching transmission system. Network management, i.e. management of the signalling and switching transmission system, on the other hand is the province of TMN. A quick comparison between the functionality of the two architectures reveals that IN could to some degree be made to fit within the framework of TMN. As we have already shown, IN can be used to implement TMN's loosely defined concept of service management, and so augment its more detailed conception of network management (which, as shown in section 4.1, exploits the management model defined as part of OSI). This becomes more obvious when we look at how TMN is modelled in terms of the logical layering of

Operations Support Systems (OSS), as shown in Figure 1. Summarising the characteristics of each layer:

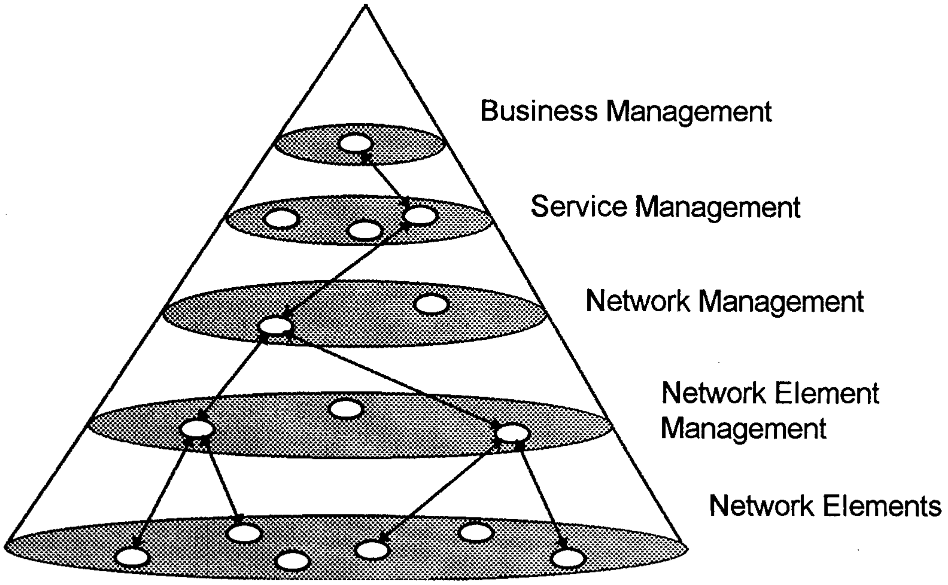

Figure 1: TMN Operations Support Systems layer model

- *Network Element Layer* : contains network element functions (e.g. modems, switches, routers, multiplexers);
- *Network Element Management Layer* : functions that manage individual network elements (e.g. equipment management and unit interconnectivity);
- *Network Management Layer* : functions that manage networked transmission systems—viz. performance, fault, accounting, configuration, and security management. [4]
- *Service Management Layer* : functions that manage services without visibility of the underlying transmission system networks (e.g. billing, verification, provisioning, inventory);
- *Business Management Layer* : functions that manage the operations of an organisation as a group (e.g. defence, telecommunications carrier, pay-TV operator, large business).

According to this scheme, the management plane functions of IN might be placed in the service management layer of the OSS layer model, with the control plane functions (call control, service control and specialised resource) situated in the network element layer.

[4] These are the five main management functions defined in the OSI reference model management standards.

4.1 Network Management

Before going on to look at how the TMN concept might be taken beyond the bounds of ITU and ISO standards, let us briefly summarise the 'standard' approach to network management. The OSI network management model shown in Figure 2 is built upon the communications infrastructure represented as the, now famous, seven layer *protocol stack* called the OSI Reference Model. Furthermore, a database, referred to as the Management Information Base (MIB), interfaces with each layer via a mechanism known as a Layer Management Element (LME). In this way the network is modelled as *managed objects* which describe physical network resources in terms of their attributes, the operations they perform, the notifications they make and their behaviour in response to operations performed on them. Finally, the management application interfaces with the protocol stack via a set of *association-oriented* protocols that reside in the application layer. These include the Common Management Information Protocol (CMIP), which is used between peer Common Management Information Service Elements (CMISE), and the Remote Operations and Association Control Protocols (ROP and ACP), which is used between peer Remote Operations and Association Control Service Elements (ROSE and ACSE). The CMISE service provides the basis for exchanging management data between managed objects: creating and deleting objects, manipulating

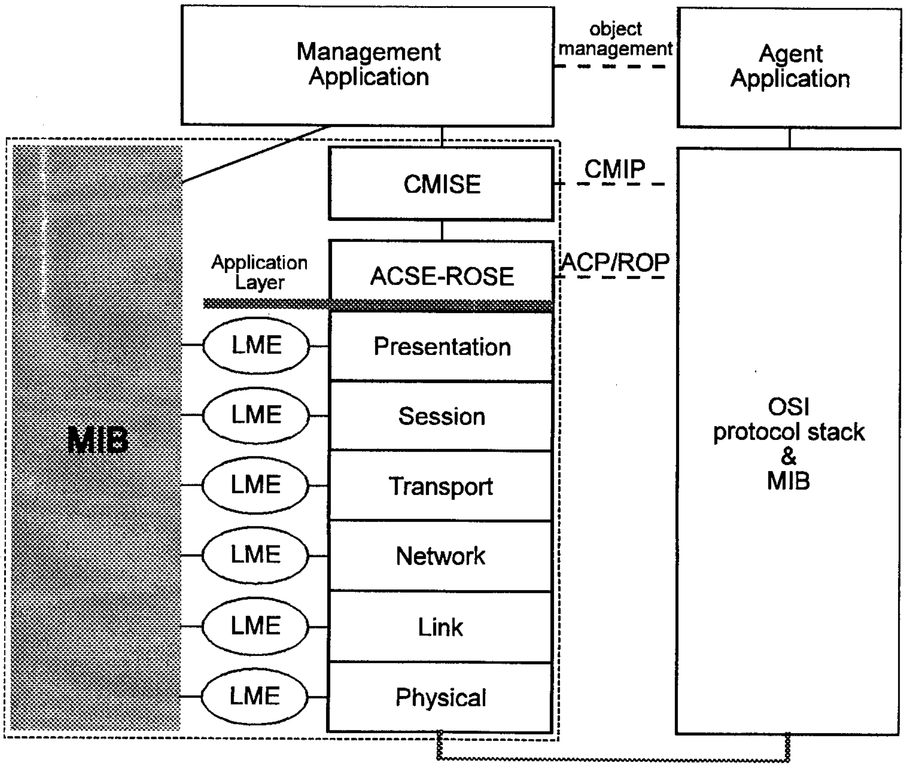

Figure 2: OSI Network Management Model

attributes and processing notifications. Assisting in this process is the ACSE service, which sets up and releases associations between managed objects, and the ROSE service, which remotely invokes operations and receives correlated responses.

The concept of an association is critical in understanding how CMIP differs from its main rival: the Simple Network Management Protocol (SNMP) defined by the Internet under the supervision of IAB. Thus, CMIP employs a *connection-oriented* transport service (i.e. one which guarantees the delivery of messages) to build 'managed' associations (i.e. relationships between objects governed by states and state transitions) between a CMISE and individual LME's. By contrast, SNMP uses a *connectionless* transport service (i.e. one in which message delivery is not guaranteed) to pass messages between a manager and its agent in a *stateless* environment. This is not the place to go into the (sometimes fierce) debate as to which is the better approach, but suffice it to say that your position is likely to have a lot to do with your attitude as to whether network management works best by controlling complex objects using robust connections, or by controlling 'scalar' objects (i.e. simple attributes) over unreliable connections. In extremely simple terms, the former makes the assumption that a network can be economically built and managed using connections that never fall over, while the latter assumes that no such network can realistically be built which is why we have network management in the first place.

Regardless of the suitability (or otherwise) of SNMP for network management, the fact remains that SNMP is hugely popular and widely implemented, and arguably likely to continue to eclipse CMIP for the foreseeable future. This fits well with the standardisation philosophy of IAB as compared with ITU and ISO: better to define an imperfect standard which has large vendor support now, than to attempt to define a near perfect standard and lobby for vendor support afterwards.[5] The SNMP architectural model is shown in Figure 3. There are obvious similarities between it and CMIP: the relationship between management system and managed system and the management protocol/s sitting on top of a communications protocol stack. The communications protocols used are part of what is known as the *Internet Suite of Protocols* (e.g. the connection-oriented transport service Transmission Control Protocol, TCP, the connectionless-mode transport service User Datagram Protocol, UDP, and the connectionless-mode network service Internet Protocol, IP). However, there are also significant differences. For one, SNMP makes use of a far smaller protocol stack. Also, missing from Figure 3 is the MIB shown in the CMIP architecture. This is in part a convention, since SNMP too has a database of management information, albeit a far simpler one. However, it also reflects a major difference between MIB's in the two systems. With CMIP, a MIB defines managed objects as highly complicated data structures that include lists of attributes, events emitted, and the imperative actions that can be carried out. By contrast, the 'scalar' objects of SNMP are similar to the attributes of CMIP objects. Furthermore, the nature of an SNMP MIB is fundamentally different to that of CMIP where managed objects are controlled via connection-oriented associations between a CMISE and individual LME's. In the case of SNMP, the collection of

[5] Whether the customer is better off as a consequence is one of those fierce on-going debates best not entered into in this paper.

managed objects is treated as a MIB as though held in an agent—objects are controlled via *datagram* (i.e. connectionless) messages passed between manager and agent in accordance with information about a device made visible by an agent through its *management instrumentation*. Put very simply, CMIP employs a 'network MIB' where SNMP employs only 'agent MIBs'.

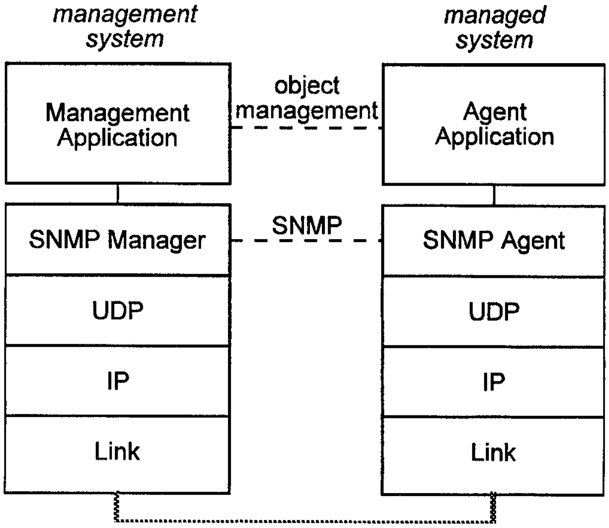

Figure 3: SNMP architecture

Numerous variations of the two main network management architectures we have dealt with here are possible. For one, a TCP/IP network might be managed by CMIP rather than SNMP by replacing the SNMP Manager and Agent in Figure 3 with CMISE running over an ACSE-ROSE layer, where the latter interfaces with the TCP/IP protocol stack via a presentation protocol known as Lightweight Presentation Protocol (LPP). [6] Of perhaps equal importance to the military is the management of emerging ATM networks. This is still a highly active area of research; however two main approaches may be identified. As a transition to the integrated network management of future ATM networks, architectures have been proposed wherein a *local area network* (based on the OSI Reference Model, for example) serves as a *data communication network* (i.e. a 'bit-pipe' transmission system) between management agents themselves and between management agents and a management application. Here, the management agents interact with managed objects in the layers of an ATM protocol stack and communicate the resultant information over the local area network. The second approach focuses on network management as an integral component of ATM networks. This is presently still in the experimental stage, and awaits much more research and standardisation work.

[6] LPP provides a mechanism for supporting OSI application services directly over TCP/IP environments.

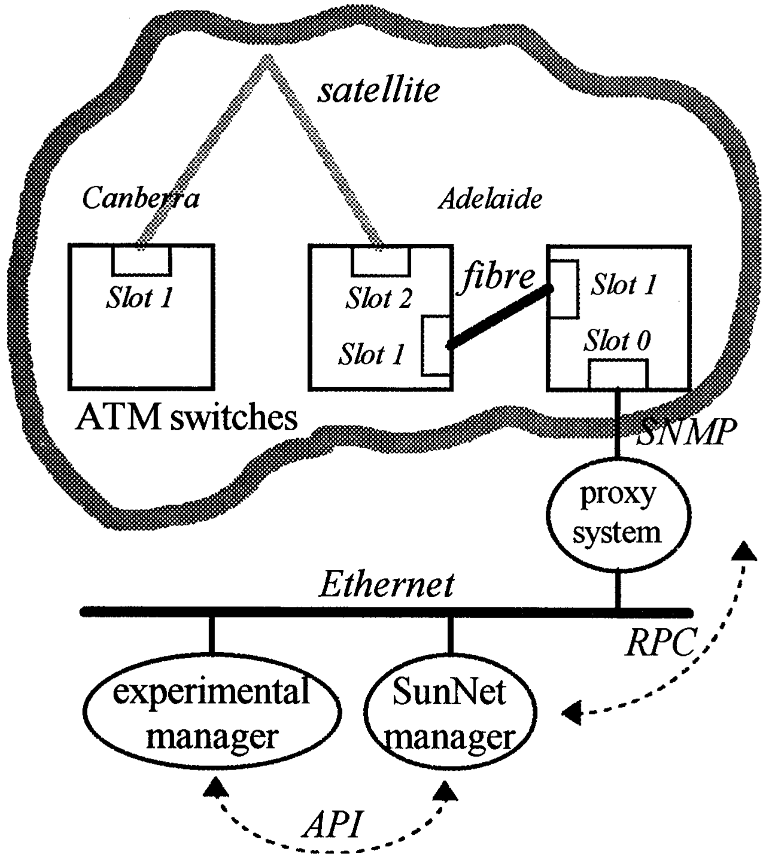

Figure 4: Network management in the DSTO Research ATM Network

One such experimental configuration is that of the DSTO Research ATM Network, as shown in Figure 4. This shows how the SNMP-based network management product SunNet [7] is used to control a small community of ATM switches. The management console (i.e. SunNet Manager) communicates with a *proxy system* via the native protocol called Remote Procedure Call (RPC) which is part of NFS, a distributed file system. The proxy in turn translates RPC into SNMP, allowing the console to be located anywhere on the Ethernet local area network and remote to any of the ATM switches. Furthermore, an experimental management application also resides on the network and interacts with the console via the Application Programming Interface (API) supported by SunNet.[8] In this way, the console serves as a *node control* device, or more accurately, a network manager that treats all the switches (both local and remote) as isolated

[7] SunNet and NFS are tradmarks of Sun Microsystems.

[8] Consistent with a *rapid prototyping* software engineering methodology, the SunNet API's, which come as C code, are encapsulated as objects using the *object-oriented design* language Eiffel.

network elements. In other words, it deals with configuration and control of one or more switches without any regard to the relationship between switches. By contrast, the experimental manager explores ways in which the community of switches might be managed as a complete ATM network. For example, the failure of a fibre transmission system may be countered with a 'fall-over strategy' that redirects traffic over satellite, and then proceeds to implement strategies to counter the resultant dramatic increase in traffic (e.g. *source policing* by configuring ATM interface cards on various workstations, via SNMP, to reduce their throughput). The DSTO Research ATM Network, then, allows researchers to play an active role in the development of ATM technology and architectures by investigating vital issues such as the impact of network management on signalling between switches and between switch and user. [9]

4.2 Service Management

As already mentioned, IN caters for service management through the functional entity called the Service Management Function. The physical system within which the SMF is implemented contains objects which manage services through the creation and modification of service parameters and data. The *service management system* needs to be accessible to a variety of groups, for example: network operators, service providers, service customers and services users. Consequently, a complicated mechanism is required to allow different groups to customise particular services according to their respective access rights. Another way of putting it is to say that service management involves looking at services in terms of a set of social aggregates (organisations, groups of individuals etc.) which each have a slightly different vested interest in a given service (some offer it, some carry it, some subscribe to it, some actually make direct use of it etc.)—and so consequently, each aggregate can be identified to as having different *claims* on a given service. The problem then, is to design sets of rights that fairly reflect claims without conflicting with one another. An associated problem is that known as *feature interaction*. This has to do with the fact that services are made up of a packaging of call processing entities called *features*. (Applying the management plane model again, it can be shown that the former problem is concerned with the management plane, whereas this problem relates to the control plane.) In the basic flow of control for call processing, features may interact in a number of undesirable ways; for example:

- a feature that is active on a call may inhibit other features from becoming active;
- multiple features may want to interpret the same signalling event in different ways.

To overcome situations such as these some sort of arbitration is required, this being the responsibility of a *feature manager* which complies with *feature interaction rules* as defined by the SMF. Service management as offered by IN, then, can be divided into the following two functions:

- *Service Negotiation*. Administration of service parameters and direct customer subscription for available services.

[9] These refer, respectively, to switch control and call control.

- *Service Creation and Deployment*. Production of services by creating feature components and feature interaction rules. Storage of service packages in a library, configuration and testing of the service package *load* (i.e. memory image) for the target node environment.

This capability is often referred to as Operations, Administration, Maintenance and Provisioning (OAM&P) of intelligent network services.

At the beginning of this section we briefly compared the functional architectures of IN and TMN with a view to the overlap between the two, and the way in which the two architectures might be integrated. This led us to the OSS layer model of TMN (refer again to Figure 1), with the service management layer provided by the service management capability of an IN architecture—i.e. its OAM&P. It is this type of integration of these two architectures that is the concern of the TINA Consortium, with its evolving goal architecture, TINA.

4.3 Distributed Systems

As we have seen in section 2, the proliferation of large-scale heterogeneous information systems raises serious problems for designers of information networks in terms of controlling complexity. A sound grounding in the better design, simulation and management of such networks is in the adoption of suitable *structuring mechanisms*—i.e. architectural models of computation and networking.

With the growing migration from locally to globally distributed systems, the traditional basic client-server model is proving to be inadequate in dealing with an explosion in complexity. The OSI Reference Model gave us the concept of *layers* containing *services* with well-defined *interfaces*. These services are further divided into *modules*, which we may then treat as distributed processes when modelling distributed systems. With the advent of *object-oriented programming*, designers of information networks have begun to turn the emphasis on interfaces and modules into a model of distributed systems based on a collection of interacting objects.

Increasingly, *object-oriented distributed systems* are competing with *client-server systems* as the architectural model of choice for networked computation. The following is a brief description of three key architectures and reference models of this type:

- *Information Networking Architecture*. This architecture from Bellcore is being touted as the successor to IN. Objects are grouped into modules called *building blocks* that provide services to one another through well defined interfaces called *contracts*. Objects can be further divided into those that facilitate interoperability between applications and those that define network resources based on various transportation technologies. The former is referred to as the *service segment* and the latter the *delivery segment*. Contracts between building blocks still make use of a client-server model, however the underlying transportation infrastructure is a distributed processing environment. [10] Specifically, the

[10] This makes the distinction between 'basic' client-server and 'distributed' client-server systems. In the case of the latter, servers can in some cases be considered to be 'objects'. However, in more fully object-oriented distributed systems, client-server relationships become 'contracts' between object interfaces—the entire architecture in such systems are thus modelled as various objects arranged according to the contracts between them.

DPE kernel supports two *levels* (i.e. architectural layers or software functions). One of these is the *information networking services level* which comprises service segment building blocks only, providing end-user service-specific functions, such as service logic and service management. The other is the *system management functions level* which comprises both delivery and service segment building blocks. Here, each delivery segment building block provides management operations on a set of managed objects based on the OSI management framework, while service segment building blocks invoke these operations via contracts. The building blocks from the two segments at this level interact via CMISE and CMIP.

- *Open Distributed Processing*. An attempt to standardise on a framework for distributed processing, or computation, is under way with ITU's ODP reference model, via the ITU-T X.900 Series of Recommendations. An interesting feature of this architectural reference model is its taxonomy of framework *viewpoints* (i.e. abstractions). These include: enterprise, information, computation, engineering and technology—taking a specification from requirements analysis through to functional specification, design and implementation. These then ultimately relate to the standard functions that are required to support computation (i.e. processing) and engineering (i.e. distribution)—or in the language of INA, the service segment and delivery segment. Furthermore, ODP defines a number of *transparencies*, which are mechanisms that hide the complexity of a distributed system infrastructure from applications developers.
- *Distributed Management Environment*. This architecture from OSF is concerned with unifying systems management (software installation, performance monitoring, configuration etc.) in heterogeneous environments. Specifically, it address issues such as: (a) consistency of user interfaces by providing a common management graphics user interface (e.g. Motif); (b)interoperability between different management systems by supporting common management protocols (e.g. SNMP, CMIP); and (c) network extensibility into potentially large heterogeneous environments by virtue of a layered network hierarchy.

DME and its simpler counterpart the Common Object Request Broker Architecture (CORBA) from the Object Management Group (OMG) have much in common with ODP, as does INA. An important distinction is that ODP is only a framework (i.e. reference model), whereas both DME and INA are specific implementations. Furthermore, INA is only concerned with a subset of ODP—viz. computation, engineering and technology viewpoints. Secondly, DME is specifically a DOMS application, i.e. it is a management system based on object-oriented distributed system technology, whereas INA aims at supporting applications in general while also incorporating service management and network management.

5. Conclusions

The complexity of evolving civil network management standards demands that serious consideration be given to the task of understanding how to integrate the management of Defence networks for improved efficiency, interoperability, and flexibility of service provision. In a military environment, specific issues arise which need to be addressed such as the security of network management information, the reliability of critical network management software, and the survivability of the network management system itself. In conjunction with civil network operators, a goal network management functional architecture needs to be identified, and a migration strategy developed which is consistent with their plans and military requirements. This should encompass issues arising from the need for each network to access the other's data and control its services so as to manage services end-to-end and optimise operations globally.

6. References

1. Ali Al-Tarafi, "Network Control and Management for Broadband Services", *Proc. ATM Broadband*, Sydney, October 1994.
2. Amatzia Ben-Artzi et al., "Network Management of TCP/IP Networks: Present and Future", *IEEE Network Magazine* , July 1990, pp. 35–43.
3. Michael Cain, "Managing Run-Time Interactions Between Call-Processing Features", *IEEE Communications Magazine* , February 1992, pp. 44–50.
4. Jock Embry et al., "An Open Network Management Architecture: OSI/NM Forum Architecture and Concepts", *IEEE Network Magazine* , July 1990, pp. 14–22.
5. Alan Lloyd, "Service and Management Aspects of B-ISDN Systems", *Proc. Australian Broadband Switching and Services Symposium 1993* , July 1993, pp. 354–362.
6. Gerhard Maegerl, "TMN and IN in the Framework of 'Intelligence in the Network'", in P. W. Bayliss (ed.), *Intelligent Networks: The Path to Global Networking* , Proc. ICCC Intelligent Networks Conference, Tampa, May 1992, pp. 316–332.
7. Natarajan and G. M. Slawsky, "A Framework Architecture for Multimedia Information Networks", *IEEE Communications Magazine* , February 1992, pp. 97–104.
8. John R. Nichol et al., "Object Orientation in Heterogeneous Distributed Computing Systems", *IEEE Computer* , June 1993, pp. 57–67.
9. Popescu-Zetelin and T. Magedanz, "Applying Open Network Provision to ISDN and Intelligent Networks", *Computer Networks and ISDN Systems 24* , 1992, 1–14.
10. David A. Pezzutti, "Operations Issues for Advanced Intelligent Networks", *IEEE Communications Magazine* , February 1992, pp. 58–63.
11. N. Truyen et al., "Telecommunications Management Network for Broadband-ISDN", *Proc. Australian Broadband Switching and Services Symposium 1993* , July 1993, pp. 337–345.

The DORIC Program: Network Management

Paul Berry and Wolf Getto

DSTO-RR-0033

DISTRIBUTION LIST DEPARTMENT OF DEFENCE	Copies

Defence Science and Technology Organisation

Chief Defence Scientist and members of the	) 1 shared copy
DSTO Central Office Executive	) for circulation
Counsellor, Defence Science, London	(Document Control sheet)
Counsellor, Defence Science, Washington	(Document Control sheet)
Scientific Adviser - POLCOM	1
Senior Defence Scientific Adviser	1
Assistant Secretary Scientific Analysis	1
Director, Aeronautical & Maritime Research Laboratory	1

Electronics and Surveillance Research Laboratory

Chief, Communications Division CCD	1
Chief, Information Technology Division - CITD	1
Research Leader, Military Communications - RLMC	1
Research Leader, Secure Communications - RLSC	1
Research Leader, Command, Control, Communications - RLC3	1
Research Leader, Military Computing Systems - RLMCS	1
Research Leader, Command, Control and Intelligence Systems - RLCCIS	1
Head, Switched Networks - HSN	1
Head, Radio Networks - HRN	1
Head, Communications Integration - HCI	1
Paul Berry	1
Wolf Getto	1

Navy Office

Navy Scientific Adviser (NSA)	1

Army Office

Scientific Adviser, Army (SA-A)	1

Air Office

Air Force Scientific Adviser (AFSA)	1

Libraries and Information Services

Defence Central Library - Technical Reports Centre	1
Manager Document Exchange Centre (MDEC) (for retention)	1
Additional copies which are to be sent through MDEC	
DIS for distribution:	
National Technical Information Centre, United States	2
Defence Research Information Centre, United Kingdon	2
Director Scientific Information Services, Canada	1
Ministry of Defence, New Zealand	1
National Library of Australia	1
Defence Science and Technology Organisation Salisbury, Research Library	2
Library Defence Signals Directorate Canberra	1
AGPS	1
British Library Document Supply Centre	1
Parliamentary Library of South Australia	1
The State Library of South Australia	1

Spares

Defence Science and Technology Organisation Salisbury, Research Library	31

Headquarters Australian Defence Force

Development Division

Director General, Force Development (Joint) - DGFD (Joint)	1
Director General, Force Development (Land) - DGFD (Land)	1
Director General, Force Development (Air) - DGFD (Air)	1
Director General, Force Development (Sea) - DGFD (Sea)	1
Director Communications Development - DCD	1
Director Communications and Information System Policies and Plans DCISPP	1

Operations Division

Director General, Joint Communications and Electronics - DGJCE	1

Acquisition and Logistics Program

Defence Materiel Division

Director General, Joint Projects Management Branch - DGJPM	1
Assistant Secretary, Communications and Info. Systems Eng. Branch - ASCISE	1
Director, Communications Engineering Development - DCED	1

Strategy and Intelligence Program

Force Development and Analysis Division

Assistant Secretary, Project Development - ASPD	1

Defence Intelligence Organisation

Deputy Director, Defence Intelligence Organisation - DDDIO	1

Defence Signals Directorate

Director, Defence Signals Directorate	1

1. Page Classification
UNCLASSIFIED

2. Privacy Marking/Caveat
(of document)

Department of Defence

DOCUMENT CONTROL DATA SHEET

3a. AR Number AR-009-224	3b. Laboratory Number DSTO-RR-0033	3c. Type of Report RESEARCH	4. Task Number ADF 92/515.1
5. Document Date 16 FEBRUARY 1995	6. Cost Code 823885	7. Security Classification	8. No of Pages 15
			9. No of Refs 11

10. Title

The Doric Program: Network Management

7. Security Classification

*		
U	U	U
Document	Title	Abstract

S (Secret) C (Confi) R (Rest) U (Unclas

* For UNCLASSIFIED docs with a secondary distribution LIMITATION, use (L) in document box.

11. Author(s)
Paul Berry, Wolf Getto

12. Downgrading/Delimiting Instructions

13a. Corporate Author and Address

Electronics & Surveillance Research Laboratory
PO Box 1500, Salisbury SA 5108

13b. Task Sponsor
DGFD(J)

14. Officer/Position responsible for

Security: ....SOESRL..........

Downgrading: ......CCD..........

Approval for Release: ......CCD..........

15. Secondary Release Statement of this Document

APPROVED FOR PUBLIC RELEASE

16a. Deliberate Announcement

NO LIMITATION

16b. Casual Announcement (for citation in other documents)

☒ No Limitation □ Ref. by Author, Doc No. and date only

17. DEFTEST Descriptors
COMPUTER NETWORK ARCHITECTURE
INTEROPERABILITY
NETWORK SECURITY
SURVIVABILITY
COMMUNICATION NETWORK
MANAGEMENT

18. DISCAT Subject Codes

19. Abstract

A characteristic of network management today is its growing diversity in the face of increasing network complexity. For one thing, we are beginning to think of electronic communication networks in terms of 'information networks', comprising networked transmission systems and networked information systems. Secondly, what used to be thought of as simply network management is now splitting into two main capabilities: network management and service management. The complexity of evolving civil network management standards demands that serious consideration be given to the task of understanding how to integrate the management of Defence networks for improved efficiency, interoperability, and flexibility of service provision.